netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2008 Issue # 24

June 13, 2008

Table of Contents

Product Focus

ASN.1 Vulnerability Scanner – The S4 ASN.1 Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the MS04-007 that could allow remote code execution.

CTO Jesper Jurcenoks of netVigilance is speaker at the HP Technology Forum & Expo 2008 in Las Vegas June 19, see
http://www.netvigilance.com/events

This Week in Review

Help to small biz from congress. IEEE working on new method. The best tools against rootkits. US covernment computers hacked from China.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.
(503) 524 5758 or sales@netVigilance.com

Top Security News Stories this Week

- **New law would bring cybersecurity help to small biz**

The U.S. Small Business Administration (SBA) could soon get a boost in helping small to mid-sized enterprises cope with information security concerns, under new legislation

being introduced in Congress that is aimed at helping users identify potential information security breaches to protect them and their customers.

Small businesses represent nearly 95 percent of all American businesses. And according to a recent Small Business Technology Institute survey, more than half of all small businesses in the United States have experienced a security breach.

Sc magazine

Full Story :
http://www.scmagazineus.com/New-law-would-bring-cybersecurity-help-to-small-biz/article/111189/

❖ Containing Internet Worms

A new method could stop Internet worms from spreading.
The spread of Internet worms could be stopped early on by using a new method to watch computers for the behavior exhibited by infected hosts, according to research recently published in IEEE Transactions on Dependable and Secure Computing. Although other methods exist to protect against worms, the new strategy is designed to minimize interference with users' normal work patterns, says Ness Shroff, a professor in the electrical-engineering department at Ohio State University, who was involved in the research. The researchers envision the technique being used in corporate networks, where it could identify computers that need to be quarantined and checked for infection.

Technology review

Full Story :
http://www.technologyreview.com/Infotech/20894/?a=f

❖ AV-Test.org releases anti-rootkit results

The results of a new study of security solutions' ability to protect users against malware hidden by rootkits has been released by AV-Test.org (http://www.av-test.org). The study tested a number of security solutions from several vendors against rootkits - programmes designed to hide files, processes or registry entries. Although they are not malicious in themselves, cyber-criminals frequently use them to hide malicious code.

Panda ActiveScan (http://www.activescan.com), Panda Security's free online scanner, detected and eliminated 86% of the malware strains that used rootkits to hide, beating online scanners from rival offerings that include Trend Micro HouseCall and Kaspersky Online Scanner. Subsequent to the test, Panda Security has released a new version of the scanner: Panda ActiveScan 2.0.

Network times

Full Story :
http://www.networktimes.co.za/news.aspx?pklNewsId=29294&pklCategoryID=196

❖ Wolf Warns Of Foreign Attacks on Computers

Rep. Frank R. Wolf (R-Va.) called yesterday for better measures to protect government computers and cellphones from cyber-attacks after revealing that computers in his office and several others on Capitol Hill had been targeted in recent years by hackers thought to be based in China.

Wolf, a champion of human rights in China and elsewhere, said at a news conference that authorities investigated the attacks on four of his computers in August 2006 and traced them to a computer in China.

Washington Post

Full Story :
http://www.washingtonpost.com/wp-dyn/content/article/2008/06/11/AR2008061102790.html

New Vulnerabilities Tested in SecureScout

- **12156 SSL supported protocol versions**

SSL is a network layer that allows privacy in communications. SSL evolved over the years to support different versions of the protocol.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gather Info** Risk: **Low**

References:

* MISC: About the risk of using invalid certificates:
http://www.rsasecurity.com/products/keon/datasheets/KWS_DS_0702.pdf
* MISC: Mozilla wiki:
http://wiki.mozilla.org/Necko:SSL_v2_Sites
* MISC: Secure_Sockets_Layer
http://en.wikipedia.org/wiki/Secure_Sockets_Layer
* MISC: What is SSL?
http://info.ssl.com/article.aspx?id=10241
* MISC: OpenSSL: The Open Source toolkit for SSL/TLS
http://www.openssl.org/

CVE Reference:

- **16945 Bluetooth Vulnerability (MS08-030/951376) (Remote File Checking)**

A remote code execution vulnerability exists in the Bluetooth stack in Microsoft Windows because the Bluetooth stack does not correctly handle a large number of service description requests. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete date; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: ms08-030
http://www.microsoft.com/technet/security/bulletin/ms08-030.mspx
* FRSIRT: FrSIRT/ADV-2008-1777
http://www.frsirt.com/english/advisories/2008/1777
* SECTRACK: 1020221
http://www.securitytracker.com/alerts/2008/Jun/1020221.html
* BID: 29522
http://www.securityfocus.com/bid/29522

CVE Reference:

CVE-2008-1453 (cve.mitre.org, nvd.nist.gov)

• 16946 HTML Objects Memory Corruption Vulnerability (MS08-031/950759) (Remote File Checking)

A remote code execution vulnerability exists in the way Internet Explorer displays a Web page that contains certain unexpected method calls to HTML objects. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: ms08-031
http://www.microsoft.com/technet/security/bulletin/ms08-031.mspx
* SECTRACK: 1020225
http://www.securitytracker.com/alerts/2008/Jun/1020225.html
* MISC: ZDI-08-039
http://www.zerodayinitiative.com/advisories/ZDI-08-039/
* BID: 29556
http://www.securityfocus.com/bid/29556
* FRSIRT: FrSIRT/ADV-2008-1778
http://www.frsirt.com/english/advisories/2008/1778

CVE Reference:

CVE-2008-1442 (cve.mitre.org, nvd.nist.gov)

• 16947 Request Header Cross-Domain Information Disclosure Vulnerability (MS08-031/950759) (Remote File Checking)

An information disclosure vulnerability exists in the way Internet Explorer handles certain request headers. An attacker could exploit the vulnerability by constructing a

specially crafted Web page. When a user views the Web page, the vulnerability could allow the attacker to read data from another Internet Explorer domain.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Medium**

References:

* MS: ms08-031
http://www.microsoft.com/technet/security/bulletin/ms08-031.mspx
* FRSIRT: FrSIRT/ADV-2008-1778
http://www.frsirt.com/english/advisories/2008/1778
* SECTRACK: 1020226
http://www.securitytracker.com/alerts/2008/Jun/1020226.html

CVE Reference:

CVE-2008-1544 (cve.mitre.org, nvd.nist.gov)

• 16948 MJPEG Decoder Vulnerability (MS08-033/951698) (Remote File Checking)

A remote code execution vulnerability exists in the way that the Windows MJPEG Codec handles MJPEG streams in AVI or ASF files. A user would have to preview or play a specially crafted MJPEG file for the vulnerability to be exploited.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: ms08-033
http://www.microsoft.com/technet/security/bulletin/ms08-033.mspx
* FRSIRT: FrSIRT/ADV-2008-1780
http://www.frsirt.com/english/advisories/2008/1780
* SECTRACK: 1020222
http://www.securitytracker.com/alerts/2008/Jun/1020222.html
* BID: 29581
http://www.securityfocus.com/bid/29581

CVE Reference:

CVE-2008-0011 (cve.mitre.org, nvd.nist.gov)

• 16949 SAMI Format Parsing Vulnerability (MS08-033/951698) (Remote File Checking)

A remote code execution vulnerability exists in the way DirectX handles supported format files. This vulnerability could allow remote code execution if a user opened a specially crafted file.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: ms08-033
http://www.microsoft.com/technet/security/bulletin/ms08-033.mspx
* SECTRACK: 1020223
http://www.securitytracker.com/alerts/2008/Jun/1020223.html
* MISC: ZDI-08-040
http://www.zerodayinitiative.com/advisories/ZDI-08-040/
* FRSIRT: FrSIRT/ADV-2008-1780
http://www.frsirt.com/english/advisories/2008/1780
* BID: 29578
http://www.securityfocus.com/bid/29578

CVE Reference:

CVE-2008-1444 (cve.mitre.org, nvd.nist.gov)

• 16950 Memory Overwrite Vulnerability (MS08-034/948745) (Remote File Checking)

An elevation of privilege vulnerability exists in the Windows Internet Name Service (WINS) in the way that WINS does not sufficiently validate the data structures within specially crafted WINS network packets. The vulnerability could allow a local attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete date; or create new accounts.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: ms08-034
http://www.microsoft.com/technet/security/bulletin/ms08-034.mspx
* SECTRACK: 1020228
http://www.securitytracker.com/alerts/2008/Jun/1020228.html
* BID: 29588
http://www.securityfocus.com/bid/29588
* FRSIRT: FrSIRT/ADV-2008-1781
http://www.frsirt.com/english/advisories/2008/1781

CVE Reference:

CVE-2008-1451 (cve.mitre.org, nvd.nist.gov)

• 16951 Active Directory Vulnerability (MS08-035/953235) (Remote File Checking)

A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 Server, Windows Server 2003, and Windows Server 2008. The vulnerability also exists in implementations of Active Directory Application Mode (ADAM) when installed on Windows XP and Windows Server 2003 and Active Directory Lightweight Directory Services (AD LDS) when installed on Windows Server 2008. The vulnerability is due to insufficient validation of specially crafted LDAP requests. An attacker who successfully exploited this vulnerability could cause the computer to

stop responding and automatically restart.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

References:

* MS: ms08-035
http://www.microsoft.com/technet/security/bulletin/ms08-035.mspx
* FRSIRT: FrSIRT/ADV-2008-1782
http://www.frsirt.com/english/advisories/2008/1782
* SECTRACK: 1020229
http://www.securitytracker.com/alerts/2008/Jun/1020229.html
* BID: 29584
http://www.securityfocus.com/bid/29584

CVE Reference:

CVE-2008-1445 (cve.mitre.org, nvd.nist.gov)

• 16952 PGM Invalid Length Vulnerability (MS08-036/950762) (Remote File Checking)

A denial of service vulnerability exists in implementations of the Pragmatic General Multicast (PGM) protocol on Microsoft Windows XP and Windows Server 2003. The vulnerability is due to improper validation of specially crafted PGM packets. An attacker who successfully exploited this vulnerability could cause the computer to become non-responsive and require a restart to restore functionality.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

References:

* MS: ms08-036
http://www.microsoft.com/technet/security/bulletin/ms08-036.mspx
* FRSIRT: FrSIRT/ADV-2008-1783
http://www.frsirt.com/english/advisories/2008/1783
* SECTRACK: 1020230
http://www.securitytracker.com/alerts/2008/Jun/1020230.html
* BID: 29508
http://www.securityfocus.com/bid/29508

CVE Reference:

CVE-2008-1440 (cve.mitre.org, nvd.nist.gov)

• 16953 PGM Malformed Fragment Vulnerability (MS08-036/950762) (Remote File Checking)

A denial of service vulnerability exists in implementations of the Pragmatic General Multicast (PGM) protocol on Microsoft Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. The protocolâ's parsing code does not properly validate specially crafted PGM fragments and will cause the affected system to

become non-responsive until the attack has ceased.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS** Risk: **High**

References:

* MS: ms08-036
http://www.microsoft.com/technet/security/bulletin/ms08-036.mspx
* FRSIRT: FrSIRT/ADV-2008-1783
http://www.frsirt.com/english/advisories/2008/1783
* SECTRACK: 1020231
http://www.securitytracker.com/alerts/2008/Jun/1020231.html
* BID: 29509
http://www.securityfocus.com/bid/29509

CVE Reference:

CVE-2008-1441 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

Microsoft Patch Tuesday

This Tuesday, Microsoft released patches for the below security issues.

- Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376)
- Cumulative Security Update for Internet Explorer (950759)
- Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)
- Vulnerability in WINS Could Allow Elevation of Privilege (948745)
- Vulnerability in Active Directory Could Allow Denial of Service (953235)
- Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762)
- Cumulative Security Update of ActiveX Kill Bits (950760)

References:
http://www.microsoft.com/technet/security/bulletin/ms08-030.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-031.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-032.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-033.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-034.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-035.mspx
http://www.microsoft.com/technet/security/bulletin/ms08-036.mspx

Apple QuickTime Multiple Vulnerabilities

"Execution of arbitrary code"

Some vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to compromise a user's system.

1) A boundary error when parsing packed scanlines from a PixData structure in a PICT file

can be exploited to cause a heap-based buffer overflow via a specially crafted PICT file.

2) An error in the processing of AAC-encoded media content can be exploited to cause a memory corruption via a specially crafted media file.

3) A boundary error in the processing of PICT files can be exploited to cause a heap-based buffer overflow via a specially crafted PICT file.

4) A boundary error in the processing of Indeo video codec content can be exploited to cause a stack-based buffer overflow via a specially crafted movie file with Indeo video codec content.

5) An error in the handling of "file:" URLs can be exploited to e.g. execute arbitrary programs when playing specially crafted QuickTime content in QuickTime Player.

Successful exploitation of these vulnerabilities may allow execution of arbitrary code.

References:
http://support.apple.com/kb/HT1991

Juniper Networks Session and Resource Control Appliances SNMP HMAC Spoofing

"Spoof authenticated SNMPv3 packets"

A vulnerability has been reported in Juniper Networks Session and Resource Control (SRC) appliances, which can be exploited by malicious people to spoof authenticated SNMPv3 packets.

The vulnerability is reported in versions 1.0.0, 1.0.1, or 2.0.0 on the C-series Controllers.

References:
http://www.kb.cert.org/vuls/id/MIMG-7ETS5Z

Cisco Products SNMPv3 Two Vulnerabilities

"Spoof authenticated SNMPv3 packets"

Two vulnerabilities have been reported in various Cisco products, which can be exploited by malicious people to spoof authenticated SNMPv3 packets.

The vulnerabilities are caused due to errors in the authentication code of multiple SNMPv3 implementations and can be exploited via specially crafted SNMPv3 packets using HMAC-MD5-96 or HMAC-SHA-96 as authentication protocol.

Successful exploitation allows to disclose certain network information or make configuration changes on a vulnerable device, but requires that the SNMP server is enabled (disabled by default).

The vulnerabilities are reported in the following products:
* Cisco IOS
* Cisco IOS-XR
* Cisco Catalyst Operating System (CatOS)
* Cisco NX-OS

* Cisco Application Control Engine (ACE) Module
* Cisco ACE Appliance
* Cisco ACE XML Gateway
* Cisco MDS 9000 Series Multilayer Fabric Switches

References:
http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

Vulnerability Resource
Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. http://www.infosyssec.org/infosyssec/

Thank You
Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com.

About SecureScout
SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.
SecureScout is a trademark of NexantiS Corporation.
netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:
Customers in America and Northern Europe contact us at info@netVigilance.com
Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net